U.S. Department of Homeland Security
Industrial Control Systems Joint Working Group[1]

Overview of the DoD Risk Management Framework and the Committee for National Security Systems Instruction 1253, Industrial Control Systems Platform IT Overlay

Daryl Haegley, OCP, CCO
Michael Chipley, PhD, PMP, LEED AP

The Department of Defense (DoD) is one of the largest owners of real estate, buildings, and Industrial Control Systems (ICS) in the United States. The DoD has over 500 installations, 300,000 buildings, 250,000 linear structures, and an estimated 2.5 million unique ICS systems.[2] As is typical with other ICS owner/operators, DoD ICS systems have become potential cyber targets, and the DoD has undertaken a number of efforts to further secure both traditional Information Technology (IT) and ICS systems. This white paper will provide an overview of a number of efforts that are underway within the Deputy Under Secretary of Defense (DUSD) and Component Installation & Environment (I&E) organizations, in conjunction with other federal and private sector partners, and lay out the next steps to ensure the cybersecurity of DoD ICS systems.

In response to changing technology, legislation, and in compliance with relevant Executive Orders, the DoD Chief Information Officer (CIO) has a number of initiatives underway:

- DoD CIO IT Enterprise Strategy and Roadmap 2010
- DoD CIO Mobile Device Strategy 2012
- DoD CIO Cloud Computing Strategy 2012
- DoD Strategy for Cyberspace 2011

These strategies are designed to provide robust, scalable, resilient, secure, and cost effective IT resources and capabilities. To achieve these objectives and benefit from the efficiencies of advanced technologies such as smart grid, smart buildings, smart meters, and smart cars, DoD needs to adopt the full National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and "sunset" the traditional Defense Information and Accreditation Process (DIACAP). As an initial part of this process, the current DoDD 8500.01E Information Assurance directive is being replaced with the DoDI 8500.01, Cybersecurity Instruction, which in turn adopts the NIST SP 800-53 RMF. Although the number of controls in NIST SP 800-53 is significantly larger than those in DODI 8500.2, it's mainly due to the fact that a single DoD control may contain many NIST controls, and the fact that NIST controls have more specificity and apply to broader number of federal policies than just the DoD's. The numerical disparity does not, however, indicate a similar increase in difficulty.

[1] http://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG
[2] DoD uses the NIST SP 800-82 definition of ICS, which in its broadest sense includes all infrastructure control systems

DoD is also a member of the Committee for National Security Systems (CNSS) and the draft cybersecurity instruction instructs DoD to use the CNSSI 1253 template[3], a companion document for the selection of controls for National Security Systems (NSS). Within DoD, ICS is defined as Platform IT (PIT), and must be evaluated for cybersecurity certification and accreditation (C&A). Working with the DoD CIO staff and the CNSS, the I&E community has proposed an expanded definition of ICS PIT that encompasses the various DoD ICS systems. Notably, the draft cybersecurity instruction provides examples of "platforms" that may include PIT, such as:

> "weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, vehicles and alternative fueled vehicles (e.g., electric, bio-fuel, Liquid Natural Gas that contain car-computers), buildings and their associated control systems (building automation systems or building management systems, energy management systems, fire and life safety, physical security, elevators, etc.), utility distribution systems (such as electric, water, waste water, natural gas and steam), telecommunications systems designed specifically for industrial control systems to include supervisory control and data acquisition, direct digital control, programmable logic controllers, other control devices and advanced metering or sub-metering, including associated data transport mechanisms (e.g., data links, dedicated networks)."

In addition, the draft cybersecurity instruction requires each system be formally designated:

> "All DoD Information System (IS) and PIT systems will be categorized in accordance with Committee on National Security Systems Instruction (CNSSI) 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are National Security System (NSS) or non-NSS."[4]

These overarching strategies and guidance will enable a more flexible and secure communication environment; however, in the interim until final publication, there remain challenges of getting smart meters installed and operational while satisfying the time-consuming DIACAP C&A requirements.

The American Recovery Reinvestment Act (ARRA) of 2009 gave the Military Services additional funding to accelerate smart meter purchasing and installation. While advantageous to collecting energy consumption data and enabling better business decisions for the I&E communities, smart meters present a network security dilemma for the DoD CIO as they are individual devices – each with an IP address that can cross-connect to other networked DoD business systems. Under the DIACAP, only the Platform Interconnect (PITI) was required to be accredited, but now with tens of thousands of meters and potentially tens of thousands of PITI's, the magnitude of the ICS cybersecurity challenge has become apparent to both CIO and facility engineers. Initial testing of the meters has revealed a number of vulnerabilities and required hardening and or disabling some system components (e.g., USB and wireless) before they could be securely connected to the network. Renowned ICS attacks - Stuxnet, Duqu, and Flame - highlighted devastating effects relevant to ICS components and systems vulnerabilities. Further, using free open source search tools such as "Shodan," one can simply reveal unsecured ICS devices and systems connected to the Internet.

In the 2010 National Defense Authorization Act, the DoD was required to develop an open protocol Energy Monitoring and Utility Control specification and ensure that it met DoD C&A requirements. In response, an update was incorporated into the Unified Facilities Guide Specifications entitled "Utility

[3] http://www.cnss.gov/Assets/pdf/Final_CNSSI_1253.pdf

[4] www.cnss.gov

Monitoring and Control System (UMCS) Front End Integration (25-10-10)." The protocol mandated open competition of ICS devices or system communications, since too many inefficacies resulted from vendor-specific protocols. Adopting an open protocol standard enables greater efficiencies but does not guarantee bolstered security.

Currently, through manual or automated means, DoD collects a large amount of energy-related data but lacks a standardized process and the integrated systems needed to systematically track, analyze, and report facility energy consumption, water use and associated expenses. In 2011, DoD began the development of an Enterprise Energy Information Management (EEIM) capability. EEIM improves DoD's ability to make informed investments regarding energy usage in the real property domain by establishing a capability to analyze comprehensive energy use and investment data and establish standardized processes and integrated systems to systematically track, analyze, and report facility energy and water use and related costs.[5] EEIM is in the final planning stages, with initial implementation scheduled to occur in 2014.

The Advanced Meter Infrastructure (AMI) (or smart meters) is fundamental to providing data needed to implement the EEIM capability. In order for all of the components of EEIM to be authorized to "ride" the DoD network, the I&E community would have to correct the lack of a standardized architecture, assessment methodology, and inventory of the ICS systems. In April 2012, to address this lack, I&E and CIO formed a Technical Working Group (TWG) and undertook the task of creating the first CNSSI 1253 ICS-PIT Overlay:

> "Security control overlays are specifications of security controls and supporting guidance used to complement the security control baselines and parameter values in the Committee on National Security Systems Instruction (CNSSI) No. 1253 and to complement the supplemental guidance in the NIST SP 800-53. Organizations select and apply CNSSI No. 1253 security control overlays by using the guidance in each of the standardized, approved and CNSS-published overlays."

The TWG delivered the first ICS-PIT Overlay to the CNSS in January, 2013, after extensive collaboration among 65 representatives spanning DoD, DHS and numerous agencies. The Overlay is both a "primer," with a standard architecture and layers diagram, and a pictorial of typical devices, sensors and actuators that enable the I&E, IT and Information Assurance (IA) staff in the field to identify and understand the operational protocols (Modbus, LonTalk, etc.), network ports, and connections. The draft version was also shared with the NIST SP 800-82 Joint Working Group and DHS's ICS-CERT Cybersecurity Protection Program for inclusion into the Cybersecurity Evaluation Tool (CSET).[6]

The initial ICS-PIT Overlay was DoD-centric and used DoD specific parameters, but was formally adopted by the CNSS in March, 2013. However, recognizing the value of the ICS-PIT Overlay, the CNNS has requested that the Overlay be generalized and made applicable to all CNSS stakeholders. The Overlay is currently being modified, and is expected to be formally submitted to the CNSS committee in May of 2013, with an expected approval and release date of July or August of the same year.

Publication of the CNSSI 1253 ICS-PIT Overlay should occur approximately at the same time as the cybersecurity instruction, with the intent that both finalized guidance documents will be integrated into the next version of the DHS CSET, 6.0, scheduled for a November, 2013 release.

[5] http://www.acq.osd.mil/ie/bei/energy.shtml
[6] http://ics-cert.us-cert.gov/Assessments

Furthermore, the Overlay is being reviewed by the NIST SP 800-82 Rev 2 Working Group for use as a model template. The NIST SP 800-82 Rev 2 publication (expected in 2014) will be based on the NIST SP 800-53 Rev 4 controls, and be updated with ICS supplemental guidance and an Overlay. An initial concept has been proposed to direct that CNSS entities use the NIST SP 800-82 Rev 2 and then remove the CNSSI ICS-PIT Overlay. This option may adequately facilitate CNSS equities and all ICS owner/operators to use a single reference standard and eliminate unique Overlays.

Once all relevant guidance has been published, the next steps to ensure the cybersecurity of DoD ICS systems include developing specific policy guidance, beginning an inventory of DoD ICS systems, and implementing an automated anomaly detection, patch and vulnerability management capability. It will also be necessary to develop and implement a workforce training program for I&E and IA professionals that integrates vulnerability and penetration testing, as well as determine the skills and qualifications for Authoring Officials to understand relevant risks of ICS system unique configuration and operational characteristics.

Authors

Daryl Haegley is a Program Manager in the Department of Defense Installations and Environment Business Enterprise Integration office. He manages the EEIM and Cybersecurity efforts, liaisons with other federal agencies on ICS issues, and was the chair of the DoD ICS TWG. In just over one year, he led the development of the CNSSI ICS-PIT Overlay, and has been instrumental in helping government and industry collaborate on securing ICS systems.

Michael Chipley is a consultant providing subject matter expert support to the Department of Defense Installations and Environment Business Enterprise Integration office. He is the lead author of the CNSSI 1253 ICS-PIT Overlay, drawing on the expertise of over 65 other subject matter experts from the DoD, DHS, and government agencies.